ETHICS AND ELECTRONIC VOTING

Chantal Enguehard

ETHICS AND ELECTRONIC VOTING

Chantal Enguehard
LINA, University of Nantes, France

Keywords*: electronic voting, transparency, confidence, election, peacekeeping*

Introduction

Voting allows citizens to participate in the democratic life of their countries or organizations (political parties, trade unions, associations, professional life, etc.): they can elect representatives or take decisions in a referendum.
Since the new millennium, electronic voting devices have appeared. In this study, we address the question of ethics and electronic voting devices.

In the first part, we will define the main properties of a democratic election, providing a typology of electronic devices and give a view on some legal documents pertaining to the matter. In the second part, the ethics of voting will be evaluated: our methodology is detailed, followed by an examination of pure paper-based elections, paperless electronic voting and verifiable electronic voting. The new concept of legally operative transparency is defined and a calendar for verifiable voting devices is proposed in the third part.

1 - Context

1.1 - Democratic election

A democratic election[1] can be seen as a way to take, collectively, a controversial decision in a limited time. When a lot of people are involved in such a decision (this is the case, for instance, when the population of a country chooses its president), the decision can not be obtained by consensus. The main idea (following a simplified model) is to tally the choices of individuals and declare elected the candidate with the largest number of votes. One criteria to evaluate if an election is successful is the capacity to maintain a peaceful climate: people who voted for a candidate that lost the election must be convinced that the election was free and fair in order to accept the defeat. If not, there is a risk of disorder that may lead to riots, and the elected candidates can be constantly challenged and their legitimacy questioned. To attain this objective of peacekeeping, elections must comply with a certain number of principles. We can cite several.
— **Secrecy**: each voter expresses her choice alone. In addition, she cannot prove how she voted because that could expose her to vote selling or coercion. It is impossible to link a ballot to the voter who cast it. The secrecy permits the voter to exercise her or his choice freely.
— **Integrity**: the results of the election faithfully reflect the will of the voters.
— **Equal suffrage**: the 'one elector, one vote' principle[2].

1 In this article, the term election includes election of representatives and referenda.

2 Every person of voting age (and not deprived of his civil rights) can vote once. There are no other criteria

— **Universality**: Each voter must be able to vote.
We make the assumption that one condition that must be met in order for an election to be defined as ethical is that the peacekeeping goal is attained, so that electors have confidence that the election had been fair. In order to be able to check if the principles cited above are respected, the election must be observable and observed. This, last but not least, is the principle of **transparency**.
We will present different definition of transparency and discuss this notion below in this article.

1.2 - Electronic voting

We consider as electronic voting any electronic system or device that ensures, at the very least, the tallying of votes. In addition, some are also used for the casting of votes, or to control voters' identity. There is a wide range of electronic voting devices that, in addition, differs from countries to countries. We present here the main families of them.

— **Voting machines** are also called **direct recording electronic (DRE) voting machines**. They record the choice of the voter who chooses by pushing a button, touching the screen or clicking on a mouse, etc. and then count the votes electronically.

— **Voting machines with a voter verifiable paper trail** (VVPT) are voting machines which print a ballot after an elector made her choice. This ballot can be verified by the voter. The ballots are collected in a ballot box in the event of needing to be manually recounted (Mercuri, 2002).

— **Internet voting** allows electors to vote directly on the internet. The voter interacts with an internet vote server to identify herself and then sends her vote. We distinguish end to end (E2E) verifiable and auditable internet voting from non-verifiable internet voting.

— **Voting kiosks**: voters can vote in any polling station. Votes are registered and tallied by a centralized electronic system.

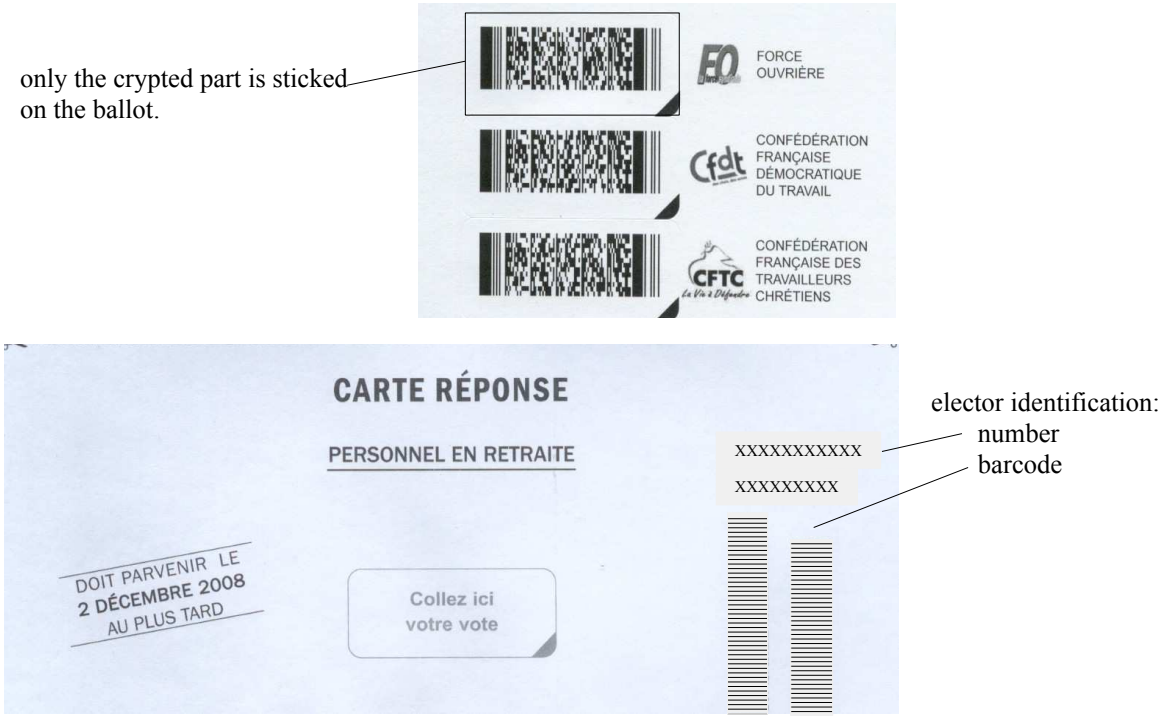

Figure 1. Ballot paper and sticky labels used in a hybrid postal election

limiting the right to vote as it was in France with the "censitaire" (a minimum income was required) or the denial of voting rights to women, still current in some countries.

— **Optical mark recognition scanners**: the voter fills her ballot with a pencil, or using an electronic device. The ballots are then inserted into a scanner that reads the ballots and tallies the votes.

— **Hybrid postal** vote (figure 1) is the use of a scanner in the case of mail voting: the voter makes her choice, sometimes by identifying herself and expressing her choice by using labels with a barcode that she sticks on the ballot. This ballot is consequently sent by mail. It will be read by a scanner.

— **Digital pens** are equipped with a camera . The ballots are printed on a special paper. When an elector votes, the camera registers its movements which will be interpreted as the expression of the choice of the elector.

— **Voting boxes** are used when all the electorate is in a same room. Each voter is provided with one of these boxes. All electors vote at the same time by choosing a number that is sent to a computer.

— **Phone**: each voter phones a special number. She identifies herself and votes by pressing the phone keys.

— **Short Message Service (SMS)**: to vote, an elector sends a message with her identification number and her choice.

We propose a simple typology (figure 2) in which each device is situated relative to three parameters:
— Voting in a voting poll (controlled environment) / remote voting;
— Votes are registered only electronically / votes are also registered on a paper ballot;
— The device controls / does not control equality by checking that each elector votes only once.

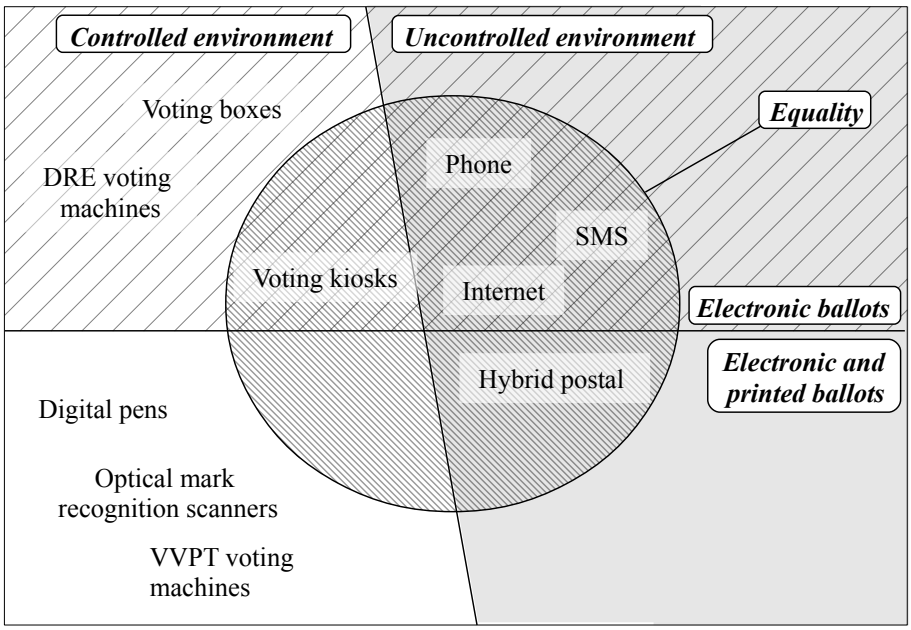

Figure 2. A typology of main electronic devices

We can see that all the electronic devices that are used in uncontrolled environment make the necessary controls to ensure equality (each elector cannot vote more than once). In consequence, they receive voter's identity and voter's choice. This situation can be perceived

as a threat against the secrecy of the vote.

1.3 - Legal documents

Two supranational organizations have produced texts on electronic voting:
— The European Commission for Democracy through Law (Venice Commission) that includes 59 member states, 47 of which being members of the council of Europe.
— The Office for Democratic Institutions and Human Rights (ODIHR) of the Organization for Security and Co-operation in Europe that is comprised of 57 participating states.

The European Commission for Democracy through Law (Venice Commission)

We first studied these documents while focusing on the question of electronic voting and transparency. Immediately, it appeared that electronic voting is very often associated with security, in the sense of the security of the electronic voting system itself, a notion that is absent when discussing paper based voting[3]. For instance, in the "Guidelines on elections" edited in 2002 (Venice Commission, 2002), the first sentence about electronic voting is « *electronic voting should be used only if it is safe and reliable* ». These notions are defined furthermore in the text: « *Electronic voting methods must be secure and reliable. They are secure if the system can withstand deliberate attack; they are reliable if they can function on their own, irrespective of any shortcomings in the hardware or software*. » In this document, the Venice Commission also recommends the use of VVAT, adding the concept of verifiability: « *In order to facilitate verification and a recount of votes in the event of an appeal* ». In addition, it gives a definition of transparency adapted to electronic voting « *the system's transparency must be guaranteed in the sense that it must be possible to check that it is functioning properly.* » and some recommendations about the counting process of an election « *counting should preferably take place in polling stations;* », « *counting must be transparent. Observers, candidates' representatives and the media must be allowed to be present.* »
In 2004, the Venice Commission produced two documents entirely on electronic voting in which are developed the themes we identified: **security** (which includes safety and reliability), **verifiability**, and **transparency**.
Four statements are entitled « *transparency* » in the Recommendation on legal, operational and technical standards for e-voting (Venice Commission, 2004).

> *20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.*
>
> *21. Information on the functioning of an e-voting system shall be made publicly available.*
>
> *22. Voters shall be provided with an opportunity to practise any new method of e-voting before, and separately from, the moment of casting an electronic vote.*
>
> *23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.*

We note that only the last one concerns the transparency of counting and that the stage of registering votes is not concerned by any of these statements.
The **verifiability** and **accountability** are based on audits and certifications to verify that « *the e-voting system is working correctly and that all the necessary security measures have been taken* ».
The security is developed through several statements detailing that the e-voting should work properly, should be audited, should be accessed by a limited number of persons , etc.
The second document is a report that addresses the question of the compatibility of remote voting (paper based or electronic) with the standards of the Council of Europe (Venice Commission,

3 When security is invoked in this manual, it is only about the protection of the poll station, by police or the intervention by the security forces in the event of trouble.

2004b). It reiterates that « *electronic voting should only be used if it is safe and reliable* » and that « *The system's transparency must be guaranteed* » in the sense that « *it must be possible to check that it is functioning properly »*. The fact that a voter has the possibility to check his or her vote immediately after casting it is presented as a measure to limit the risk of fraud. This report insists on the importance of taking measures to ensure that the principle of secret suffrage is protected.
In 2010, the Venice Commission published a handbook on e-voting (Venice Commission, 2010) which develops the key steps in the implementation of e-enabled elections. Again, it is repeated that « *without transparency states cannot guarantee that an e-enabled election was conducted according to the democratic principles of free and fair elections.* » One year later, two Guidelines on Certification of E-voting Systems (Venice Commission, 2011) and on Transparency of E-enabled Elections have been published (Venice Commission, 2011b). Certification is presented as a key element to reinforce citizens' confidence in the security and reliability of e-voting systems. Transparency concerns the access to reports by authorized persons (international observers, stakeholders for instance), the observation of the testing of the system and the use of a second medium that is software independent to control the results. Finally, a new definition of transparency is provided : « *the concept of determining how and why information is conveyed through various means.* »
It appears that, since 2002, the Venice commission has been organizing the legal environment in order to spread electronic voting systems.

The Office for Democratic Institutions and Human Rights (ODIHR)

The ODIHR has encountered electronic voting systems during its election observation missions and, at least since 2005, appreciates that electronic-voting systems with no voter-verified paper audit trail or other manual-audit capacity are « *possible problems to be aware of* » because they are challenges to the transparency and accountability of an election process (ODIHR, 2005), (ODIHR, 2010).
In 2013, the ODIHR edited a Handbook For the Observation of New Voting Technologies (ODIHR, 2013). This manual declares :

> *« Transparency is a cornerstone of the OSCE election-related commitments, as it is necessary to verify that elections take place in accordance with the law and with democratic principles. Election observation is a key aspect of transparency, recognized by paragraph 8 of the Copenhagen Document. Political parties, candidates and observers should have the opportunity to observe the work of election authorities at all levels, and especially the voting, counting and tabulation processes. »*

This handbook outlines that observations must be meaningful and that this is not the case when observing voters and officials operating machines. It advocates that observers should have full access to documentation about the system, including certification and testing reports.
Concerning security issue, the manual remarks that « *a key difference [with paper-based voting] is that attacks on NVT may require technological skills and significant resources not possessed by the typical voter to be detected or observed.* » and advises that observers should verify that robust security measures against potential threats have been taken. These measures are not listed exhaustively, but a few examples are given, such as, in the case of DRE voting machines, controlling that USB ports are not easily accessible in order to prevent physical tampering, storing and transporting devices in a secure manner under defined protocols.

For devices that are connected to the Internet, the manual insists on the possible loss of votes

and the prevention against illegitimate access or the possibility that individuals who have access to the system encounter the opportunity for internal manipulation. Again, some security procedures are advocated that must be « *both effective and fully implemented* ». In addition, some measures should be adopted to guard voters' computers against possible attack that may, for instance, change their choice or steal their usernames and passwords.
Testing the system is considered as important when considering security measures, even if it is also explained that « *testing is never a guarantee that the NVT [new voting technology] system is fully secure or that it will work properly on election day.* »
The manual gives also some directions in order to evaluate the certification process (which is prior to the vote) and the process of verifying the results: post-election audit, collection and counting of ballots for devices with printed ballots[4].

Transparency is then redefined: it concerns access to documentation and to the source code, observation of the electronic voting process, of the activities of election administrators, vendors, of the process of certification, testing and auditing, etc. This new definition contrasts with the necessity of meaningful observation that stands at the beginning the document and that is illustrated by an example focusing on the observation of the counting process in progress:

> *« in paper ballot systems counting cannot be considered transparent if observers are present during the counting but are kept at such a distance that they cannot see the content of ballots and cannot verify that votes are being counted honestly.*

3 Evaluating the ethics of electronic voting

3.1 Methodology

As stated Michael Saward (2003), « *we need a fresh view of democratic theory* » in which « *democratic principles are primarily thing we* ***do***[5]*, rather than things or statuses that are conferred* ». Following this direction, we will examine the reality of several voting devices to determine if they are transparent. Our strategy will be to develop a worst-case scenario in which security breaches (fraud or unreliability) would cause the modification of a vast amount of votes. We will then try to answer the question: would these discrepancies have been seen or stayed invisible? We will focus on the two stages of registering votes and tallying them.
In addition, we will consider if the legal texts we presented effectively address this problem.
Thus, we will focus on transparency and will not investigate the security of electronic voting because we previously proved that a « promise of security is not able to compensate for the loss of direct transparency. » (Enguehard, 2014)

3.2 Pure paper-based elections

We did not present pure paper-based elections that do not use any electronic device to register or tally the votes in detail because this is not the scope of this article. Nevertheless, we will examine this family of elections in order to compare it with electronic approaches
There are many different paper-based voting organizations, we describe here a simplified model: The electors vote with paper ballots (chosen inside a booth and slipped into an

4 Curiously, it is stated that « *For audits, it is likely that only a certain percentage of paper records will be checked* » while it should be obviously more accurate to check all the paper records.

5 The author uses bold characters in its own article.

envelope to keep the secrecy of the vote). Each elector then deposits her envelope in a voting box. The fact that an elector did not vote before is controlled in order to respect the unicity principle (for instance, each voter signs on a register). At the end of the voting period, the ballots are counted publicly, i.e. under the eyes of the public.
Within this organization, all the information is registered on neutral material: ballots are made in paper printed with ink and could not modify themselves; the ballot box is made of wood or transparent plexiglass (in France). The neutral property of the material used to register the votes is crucial: even if the stage of the voters making their choice cannot be observed, if the ballot box has been properly watched, it is certain that it contains all the ballots deposited by the voters without any change. The tallying being processed publicly by several persons is transparent in the sense of acting democracy: people can see the counting and sometimes (in France for instance) participate in this operation.

Our worst-case scenario can now be examined. A first possibility to modify a vast amount of votes could happen by altering the content of the voting box (or by exchanging the voting box with another one) during the election period. The second possibility takes place during the tallying. The opening of the voting box represents an opportunity to maliciously change a group of envelopes by another one. Again, this stage must be closely monitored by the people present. If this is the case, the fraudster can be caught[6].
It appears that the possible undermining of the integrity of the election could occur with a great magnitude only if all the persons that are present in the voting station during the fraud conspire with the fraudster. These threats can be thwarted by the presence of several persons belonging to different parties, that constantly oversee that there is no unauthorized tampering with the voting box or during the tallying. We remark that these people who ensure the smooth running of these two stages by their attentive presence do not need high qualifications in any subject.

3.2 - Paperless electronic voting

Paperless electronic voting includes all devices used in elections without any ballot paper: DRE voting machines, non-verifiable internet voting, voting boxes, voting kiosks, voting by phone or by SMS.
All these electronic devices have in common that the choices expressed by the electors are transformed in order to be registered and then tallied. For instance, with DRE voting machines, an elector votes by pressing a finger on a button, this strength is converted into an electrical signal which is then converted into an electronic information expressed using the binary base[7]. Finally, all these pieces of information that represent ballots will be transformed again during the tallying phase to produce some election results. These operations are done at an electronic level that cannot be directly observed by human eyes. These processes could malfunction because of a bug or a fraud and produce electoral results that do not reflect the sum of the voters'choices.

Would it be possible to know if some malfunctioning happened? Three possible pathways can be followed:
— Printing a log file
The electronic device could print a record of its activities which allows to follow and check the

6 Examples are not rare. We can cite the failed attempt of fraud that happened during parliamentary elections in Perpignan, France in 2012. The president of a polling station added some signatures on the signing register. He was found with several envelopes with ballots hidden in his pockets and his socks. The election had been canceled and the fraudster sentenced (Le Monde, 2011).

7 Encoded with the 0 and 1 symbols.

transformations from each vote from registering until the tallying. This approach, very common when computing, is the production of a log file. Unfortunately, this file will lead to know each elector's vote and is therefore not suitable to a free election.

— Testing

Some tests can be done. But testing a device before or after its real use could not guarantee that it functions properly during the election period. In computer science the limits of the testing procedures are well known: it is impossible to test all the possible interactions between users and a computer and some behavior could change in function of external parameters such as, for instance, the calendar.

— Proving a program

Proving a program is a mathematical method that virtually takes into account all the possible interactions between a program and its environment. This approach can be followed for a program, but is not possible, at this point of the computer science, to prove an entire system composed with different hardware and software parts. We can consider DRE voting machines which are the simplest electronic voting devices: some parts of the device may be modified during the election period (for instance, a micro-code that changes the tallying program could be injected when plugging a printer and be self-erased after the tally). Of course, this approach is completely unsuitable for voting devices that take place in uncontrolled environments: electors' phones or computers cannot be checked.

The testing or proving approaches also encounter another difficulty: checking that the program which is working (the executable program) during the election corresponds to the program that has been tested/proved[8] is a difficult problem that does not have any robust solution at this moment. That's why the access to the source code by the public or an audit commission should not be presented as a measure that enhance the transparency of the election.

We conclude that a malfunction could occur during an election and stay invisible, even if a large amount of ballots are modified by this malfunctioning.

This analysis leads to questioning the auditing approach that is strongly encouraged by the Venice Commission and the ODIHR. Audits can only test the device, or a part of it, observe some pieces of programs and be informed of some organizational details about the companies that build and sell e-voting devices. These investigations are not sufficient in order to find all the potential flaws that could jeopardize the electoral results, including those that could affect an important part of the ballots, while staying undetected.

Paperless voting devices are an opaque mode of voting in the sense that it is impossible to know if the transformation of the ballots changed the choices expressed by the voters **during an election**[9]. These devices offer neither transparency to the electors, nor anybody else: the candidates, the official members of polling stations, the technicians who manage the voting system, the judge that should intervene in a case of electoral disputes, etc., or any independent authority that audited the software. In addition, it is common that the authority in charge of audits only produces reports which are not public because of the protection of commercial and industrial property. It constitutes a second opacity. **A double opacity is not transparency.**

A French story

In France, the audit reports about the voting machines that are used since 2004 by the electorate of some cities (Enguehard, 2013) were not accessible. After a legal dispute one of

8 The interpreter or the compiler used to transform the source code into an executable program can also be flawed.

9 Enguehard and Lehn (2009) compares in detail three remote voting methods: postal voting, internet voting and hybrid postal voting and concludes that « *that the automatisation of treatments combined with the dematerialisation of the objects used during an election tends to substitute visible vulnerabilities of a lesser magnitude by invisible and widespread vulnerabilities.* »

these reports, concerning the Nedap voting machines authorized in France, had been provided to the litigant. It revealed that the devices have been authorized despite not complying with several criteria defined by a decree. Even if these discrepancies were to be judged as minor, the observation mission of the OSCE noted that « *This raised concerns that the certification companies have too much discretion in determining the acceptable amount of variance in meeting each certification criteria and in determining whether some criteria are relevant at all.* » (ODIHR, 2007)

3.3 Verifiable electronic voting

Because paperless electronic voting is not transparent, and that any major flaws affecting the electronically registered ballots or their tally could remain invisible, some researches have been tackled to specify the concept of verifiable electronic voting (Gharadaghy, Volkamer, 2010). Two verification points have been defined:
– Individual verification: each voter checks that her vote had been rightly encoded, registered and tallied.
– Universal verification: anybody can check that only legitimate votes have been recorded and tallied, and that this tally is accurate.

We will examine these two stages and then bring a legal analysis.

Individual verification

When the voter uses a digital pencil or marks her ballot paper herself, we can consider that she checks that her vote had been rightly encoded. But she gets no information about the registration and the count of her vote.
– Individual verification with VVPT
When using a VVPT voting machine, the voter does not produce her ballot paper herself: a ballot is printed by the voting machine, and the voter is invited to check if the printed information is the choice she expressed when pressing a button. She can confirm or cancel her vote. Following confirmation, the ballot is then conveyed to a ballot box whose content could be checked during the universal verification step. Again, a voter gets no information about the registration and the count of her vote.
This individual verification step is crucial because if the ballot conveyed in the ballot box does not correspond to the voter's choice, the universal verification would be useless. Unfortunately, it has been observed that many voters do not check the printed ballot that is presented (Herrnson, 2006): « *Despite all the publicity given to the paper trail issue, voters seemed largely to ignore the paper record.* »
– Individual verification with an "end to end auditable and verifiable" (E2E) internet voting system
As far as we know, the Hélios voting system (Adida, 2009) is the only internet voting system that was developed in order to be "end to end auditable and verifiable". It allows an elector to test if an encrypted ballot conveys her choice. But she cannot check the ballot she sent to the centralized computer (that receives all the ballots) because a voter must not get any proof of her vote that would expose her to coercion.
The system sends to each elector an electronically signed document that allows to check that a vote has been tallied.

Universal verification

– Universal verification of electronic voting devices with paper ballots (VVPT, digital pencil, optical mark recognition scanner or hybrid postal voting)
The universal verification is the recount of all collected ballot papers. Usually, the recount concerns only a part of the devices that have been used. Thus, some of them won't have their results checked. The time at which the devices to be checked are designated, and the organization of the checking must be precisely defined in order to get a credible verification. For instance, devices to be checked should be chosen after the voting period (to not give any clue about the devices that won't be checked) and the recount should take place immediately, in the polling station, without moving the voting box.
– Universal verification with an E2E internet voting system
Some cryptographic algorithms allow to achieve the tally of electronic ballot without accessing the identity of the voter associated with each ballot (Gharadaghy, Volkamer, 2010). Such verification can be done with Hélios but this complex operation is not accessible to all electors.

Legal analysis

The individual and universal verifications can lead to encountering some flaws, but would such flaws be taken into account during a legal dispute? The verification stages we presented above have been defined by computer scientists that are familiar with bugs: if the testing of software does not give the expected results, an error must be searched and corrected.
But, in the case of elections, this is a judge that decides if a voting device was flawed, not computer scientists. The individual verification procedure allows a voter to notice a flaw, but she could not prove it. The voting device is more transparent than a non-verifiable voting device, but this transparency could have no legal consequence: even if a large amount of voters were to encounter some changes in their ballot, they could not present any proof of their observation[10], and thus electors will carry on voting on this voting device. As a large part of the voters don't check their vote, the voting device could have registered a lot of ballots that do not meet the voter's choice and not been declared as faulty.
The universal verification of electronic voting devices with paper ballots is also inadequate for a legal evaluation because the judge needs to possess some statistical abilities to extrapolate the verification results obtained on a few devices for the entire group of devices that have been used (but not all verified).

Because of these problems we define the new concept of *legally effective transparency* and introduce some additional controls that concern verifiable voting devices and that constitute a *calendar for verifiable voting devices*.
– Definition:
The *legally effective transparency* of a voting device exists if any report of a flaw during an election is accompanied by the production of a material proof that could be taken into account by a justice court.
– Calendar for verifiable voting devices
As we explained, it is crucial that the voters really check their vote in order to avoid that a flaw modifying many ballots would stay legally invisible. It appears necessary to define a new calendar that takes into account these controls. This calendar is divided into several steps:
1. Electors make their choice.
2. Electors check that their choice has not been changed and has been tallied.
3. A temporary tally is calculated, based on the checked ballots (non checked ballots are not taken

10 In addition, this situation could also make some rumors rise, undermining the confidence in the electoral system.

into account).

4. Universal verification is processed.
5. Definitive results are claimed.

These suggestions should be evaluated and completed. There is a need for new research studies to define points of control in order to achieve the *legally effective transparency.*

Conclusion

In this article we investigate transparency because it is the cornerstone of democracy. Many more subjects should be studied. In particular the expected benefits of electronic voting, often claimed, should be evaluated.
Accessibility is supposed to be enhanced (in France, people are supposed to be able to vote alone on voting machines, whatever handicap they have), but some studies suggest the contrary, even with people without any handicap (Michel, de Abreu, Brangier, 2007), (Braconnier, Dormagen, Rocha, 2013). The capacity of increasing turnout is in discussion (Beckert, Lindner, Goos, Hennen, Aichholzer, Strauß, 2010): Internet voting would favor the participation of people who have a tendency to vote, but would not involve people who do not vote except « *a"curiosity effect" which can appear when i-voting is used for the first time* ». The lower election administration costs are also in question. In Belgium it appears that electronic voting costs more than 1,37 euro per elector while paper based voting costs only 0,1 euro per elector (Sirlereau, 2013). A French senatorial report also outlined also the necessity to evaluate such costs and also environmental costs (Sénat, 2014). Even the improvement of the accuracy of counting should not be accepted as an obvious fact. A study conducted in France (Enguehard & Graton 2014) compared the number of votes and number of signatures on the signing sheet of more than one hundred thousand poll stations for all the political elections from 2007 to 2012. It showed that these two numbers, which should be equal in a polling station, are sometimes different, and that these differences are 3 to 5 times more frequent when voting machines are used compared to paper-based voting.

DRE voting machines have been used since 2004 in France. In 2014, local elections took place in March. At least six legal disputes on the use of DRE voting machines[11] have begun, even if such disputes have never led to the cancelling of an election. The election results appeared strange to people: too regular amongst the polling stations, or too close to the last election results, etc. For the parliamentary election in 2012 French living abroad could vote by internet in 11 districts: five legal disputes on the electronic voting subject arose. This increasing number of legal disputes may mean that, because of the non-transparency, the confidence in the electoral system is decreasing.

It appears that electronic voting devices that are used at the present time could allow for some massive flaws to occur without any legal treatment of these facts, even when they are verifiable electronic devices. This lack of transparency could undermine the public confidence and lead to political and social disorder by affecting the peacekeeping role of transparent elections.

Decisions about electronic devices should consider the double question: what are the risks of using electronic voting devices? / what are the risks of not using electronic voting devices? The reality is brutally different: electronic voting is a market that some like to enhance to get

11 In Marignane, Orange, Palavas-les-Flots, Saint-Pol-sur-mer, Sèvres and Villeneuve-le-Roi.

profits[12].

References

Adida, B. (2008). Helios: Web-based Open-Audit Voting. 17th usenix security symposium. San José, CA.

Beckert, B. Lindner, R. Goos, K. Hennen, L. Aichholzer, G. & Strauß, S. (November 2011). E-public, E-Participation and E-Voting in Europe - prospects and challenges. Final Report.

Braconnier, C. Dormagen, J.-Y. & Rocha, D. (2013). Quand les milieux populaires se rendent aux urnes - Mobilisation électorale dans un quartier pauvre de Brasilia. Revue Française de Science Politique. Page 487 à 518. vol.63/3. ISSN 0035-2950

Enguehard, C. & Lehn, R. (July 13, 2009). Vulnerability analysis of three remote voting methods. XXI IPSA World Congress of Political Science, RC10 Electronic Democracy - Dilemmas of Change?. Santiago, Chile.

Enguehard, C. (30 juillet 2013). Utilisation des machines à voter en France entre 2004 et 2012. Observatoire du Vote.

Enguehard, C. (2014). Internet Voting: situation, questions and trends. in "Politics and Policy in the Information Age", edited by Jonathan Bishop, published by IGI Global.

Enguehard, C. & Graton, J.-D. (2014). Machines à voter et élections politiques en France : étude quantitative de la précision des bureaux de vote. Cahiers Droit Sciences et Technologie, CNRS editions. (to be published)

European Commission for democracy through law (Venice commission). (July 2002). Guidelines on elections.

European Commission for democracy through law (Venice commission). (September 2004). Legal, operational and technical standards for e-voting - Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum.

European Commission for democracy through law (Venice commission). (12-13 March 2004). Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe.

European Commission for democracy through law (Venice commission). (2010). E-voting handbook.

European Commission for democracy through law (Venice commission). (November 2011). Guidelines on Certification of E-voting Systems.

European Commission for democracy through law (Venice commission). (November 2011). Guidelines on Transparency of E-enabled Elections.

Fleisher, L. (7th of April 2014). Microsoft Co-Founder Allen Bets on Online Voting; Funds Scytl. WJD. Retrieved from http://blogs.wsj.com/digits/2014/04/07/microsoft-co-founder-allen-bets-on-online-voting-funds-scytl/ (consulted the 14th of April 2014).

Gharadaghy R. & Volkamer, M. (July 21st - 24th, 2010). Verifiability in Electronic Voting Explanations for Non Security Experts, 4th International Conference EVOTE 2010, p. 151-162, Bregenz, Austria.

Le Monde. (21 décembre 2011). Fraude à la chaussette : un an avec sursis pour l'auteur. Retrieved from http://www.lemonde.fr/politique/article/2011/12/21/fraude-a-la-chaussette-un-an-avec-sursis-pour-l-auteur_1621239_823448.html (consulted the 14th of April 2014).

Mercuri. R. (October 2002). A Better Ballot Box?" IEEE Spectrum Online, vol.39, n°10, p.46-50.

Michel, G., de Abreu, W. & Brangier, E. (21-22 June 2007). Electoral Ergonomic Guidelines to Solve the

12 Paul Allen's venture-capital fund will invest $40 million in Scytl, an entreprise that develops and sells internet voting (Fleisher, 2014).

Interference of new Technologies and the Dangers of their Broader use in Computerised Voting. 7th European Conference on e-Government, p.337-348, Den Haag, Netherlands.

Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe. (2005). Election Observation Book. fifth edition. ISBN 83-60190-00-3.

Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe. (4th of October 2007). France Presidential Election 22 April and 6 May 2007 - OSCE/ODIHR Election Assessment Mission Report.

Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe. (2010). Election Observation Book. sixth edition. ISBN 978-92-9234-778-9.

Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe. (2013). Handbook For the Observation of New Voting Technologies.

Saward, Michael. (2003). Enacting Democracy. Political Studies, 51: 161–179. doi: 10.1111/1467-9248.00418.

Sénat. (9 avril 2014). Rapport d´information n°445 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le vote électronique, par Alain Anziani et Antoine Lefèvre, sénateurs.

Sirlereau, M. (10 avril 2014). Communes vs Paul Furlan: un bras de fer dû au coût du vote électronique. rtbf.info. Retrieved from http://www.rtbf.be/info/belgique/detail_communes-vs-paul-furlan-un-bras-de-fer-du-au-cout-du-vote-electronique?id=8243434 (consulted the 14th of April 2014).

I specially thank John Johnson and Charlotte Rowe who kindly reviewed this article.